



A Deeper Level of Network Intelligence: Combating Cyber Warfare



Greg Kopchinski
Director, Product Management
Bivio Networks Inc.
www.bivio.net

This information is provided for your review only and is not for any distribution. Any reproduction, modification, distribution, transmission, display or republication of the content is strictly prohibited.

©2010 Bivio Networks, Inc.

People Rely on Internet

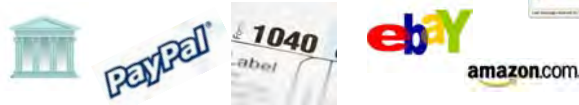
Business / Professional Use



Personal / Social Use



Financial Transactions



©2010 Bivio Networks, Inc.



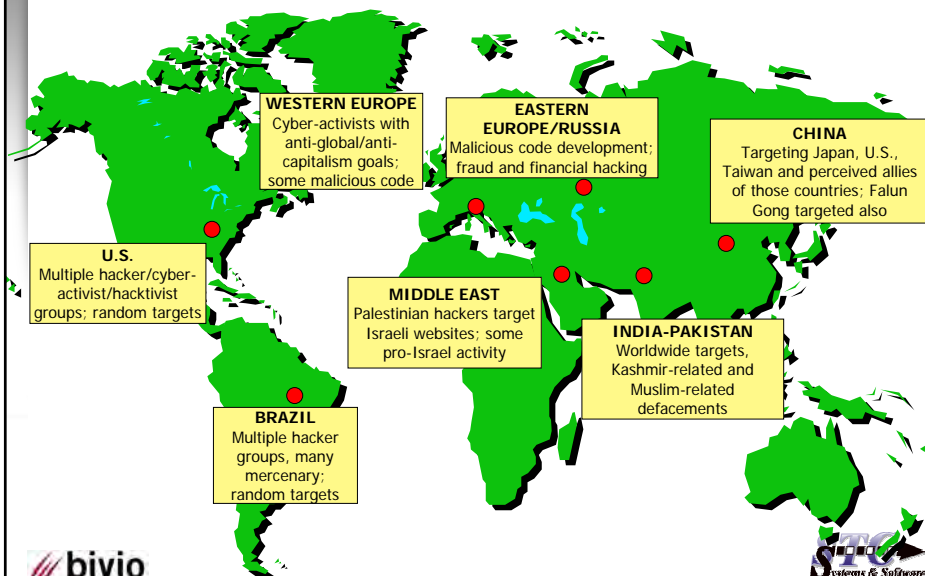
Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE APR 2010		2. REPORT TYPE		3. DATES COVERED 00-00-2010 to 00-00-2010	
4. TITLE AND SUBTITLE A Deeper Level of Network Intelligence: Combating Cyber Warfare				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Bivio Networks Inc,4457 Willow Road, Suite 200,Pleasanton,CA,94588				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES Presented at the 22nd Systems and Software Technology Conference (SSTC), 26-29 April 2010, Salt Lake City, UT. Sponsored in part by the USAF. U.S. Government or Federal Rights License					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 12	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

A Hacker's Opportunity is Target Rich!

- /// Enterprise
 - Personal
 - Credit Card
- /// Government
 - Military secrets
 - Nuclear Information
 - Medical Records
 - Criminal Records
 - Classified Secrets and Information
 - Control of Physical Infrastructure
 - Power
 - Electrical
 - Water



Hacking Hotspots and Trends



Happening Now!

- Twitter DDOS
- DDOS attacks in Estonia
- Attacks on Booz Allen Hamilton
- Breach of defense contractor computers that let hackers get at information on the Joint Strike Fighter
- Power grid compromised
- Repeated attacks on .gov websites
- Real growing threat of cyber terrorism



©2010 Bivio Networks, Inc.



5

Exploitation Evolution

- While we look at the evolution trend, it should be noted that the less severe exploits have not gone away. They still exist today and have even increased in numbers. The problem is that we also have to deal with exploits that now affect our national security.

Experimentation / Notoriety

Hactivism / Defacements

Criminal Enterprise

Espionage / Cyber Terrorism



©2010 Bivio Networks, Inc.



6

Threats Today

- /// **Malware**
 - Worms
 - Trojans
 - Rootkits
 - Spyware
- /// **Botnets**
- /// **Remote & Local Exploitation**

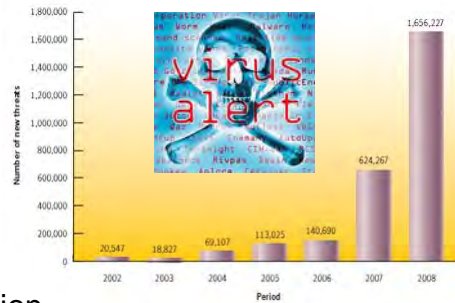


Figure 15. New malicious code signatures
Source: Symantec

Good News: New Government Initiatives Underway!



©2010 Bivio Networks, Inc.



7

CNCI Overview



The Comprehensive National Cybersecurity Initiative

- /// Cybersecurity has been called “one of the most urgent national security problems facing the new administration.”¹
- /// The CNCI “establishes the policy, strategy, and guidelines to secure federal systems.”²
- /// A program called to unify agencies’ fragmented approach to cyber security within the federal government.

(1) Center for Strategic and International Studies, Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency (2008).

(2) Department of Homeland Security, Fact Sheet: DHS 2008 End of Year Accomplishments (Dec. 18, 2008), http://www.dhs.gov/xnews/releases/pr_1229609413187.shtm.



©2010 Bivio Networks, Inc.



8

12 Main Components of the CNCI

- ✦ Trusted Internet Connection
- ✦ Intrusion Detection
- ✦ Intrusion Prevention
- ✦ Research and Development
- ✦ Situational Awareness
- ✦ Cyber Counterintelligence
- ✦ Classified Network Security
- ✦ Cyber Education and Training
- ✦ Implementation of Info Security Technologies
- ✦ Deterrence Strategies
- ✦ Global Supply Chain National Security
- ✦ Public/Private Collaboration



Two Initiatives of CNCI

- ✦ Einstein 2
 - *EINSTEIN 2 capability enables analysis of network flow information to identify potential malicious activity while conducting automatic full packet inspection of traffic entering or exiting U.S. Government networks for malicious activity using signature-based intrusion detection technology*
- ✦ Einstein 3
 - *The goal of EINSTEIN 3 is to identify and characterize malicious network traffic to enhance cybersecurity analysis, situational awareness and security response. It will have the ability to automatically detect and respond appropriately to cyber threats before harm is done, providing an intrusion prevention system supporting dynamic defense.*

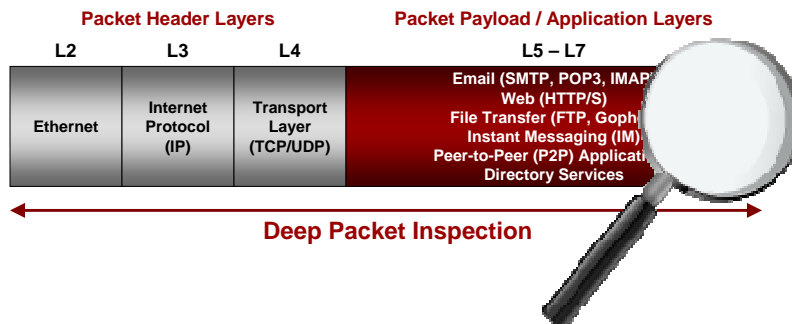
A Transforming Network

- ✦ Explosion in usage, applications, devices, protocols
- ✦ Basic networking problems remain
 - Security
 - Information assurance
 - Cyber defense
 - Awareness
 - Control
- ✦ Network role transition from connectivity to policy
- ✦ Key Enabling Technology: **Deep Packet Inspection**

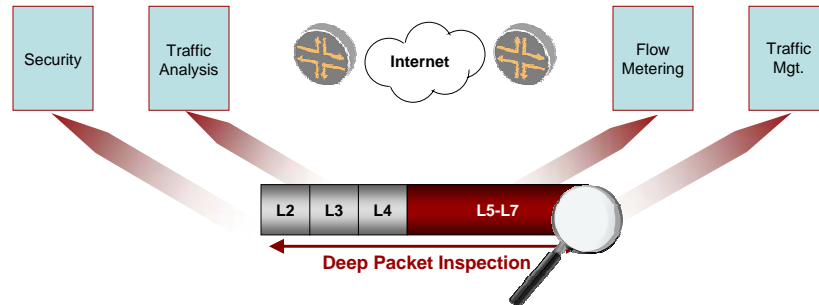


What is Deep Packet Inspection (DPI)?

- ✦ Set of technologies enabling fine-grained in-depth processing of network traffic
- ✦ Not a solution or an application!



How is DPI used?



Deep packet inspection is used for a variety of protocol-aware networking functions including:

- Prevention of security violations
- Statistical traffic analysis
- Flow metering
- Content-based billing

Cyber Security: Why DPI?

- ⚡ L3/4 analysis clearly not granular enough
 - Source/Destination often insufficient or totally irrelevant
- ⚡ Most information including viruses, worms, and bots is in the payload
 - Deeply embedded
 - Context dependent
 - Dynamic
- ⚡ Tunneling makes outer protocols/headers insufficient
- ⚡ Correlation between flows and payload often crucial
- ⚡ Threats are real-time & dynamic; response must be as well
 - DPI is real-time networking analog to off-line analysis
 - Dramatically shortens threat identification and response

Example DPI-enabled Applications

AMP



SNORT®

- ❑ Intrusion Detection and Prevention
- ❑ Network Flow Analysis
- ❑ Data Leak Prevention
- ❑ Network Monitoring
- ❑ Data Retention
- ❑ Web Content Control
- ❑ Network Forensics



YAF



BarnYard




©2010 Bivio Networks, Inc.




15

DPI Applications Requirements

Development

- Prefer Linux for networking applications 
- Limited only by developer's imagination and ability to code
- Evolve and change applications with new requirements
- Develop independent of underlying platforms

Deployment

- Provide same operational environment – Linux 
- Insulate the applications from networking delivery infrastructure
- Offer appropriate amount of compute power for application to handle the offered "speeds and feeds" (10Gbit, OC-192, beyond)
- Run multiple applications on the same "speeds and feeds" pipe



©2010 Bivio Networks, Inc.



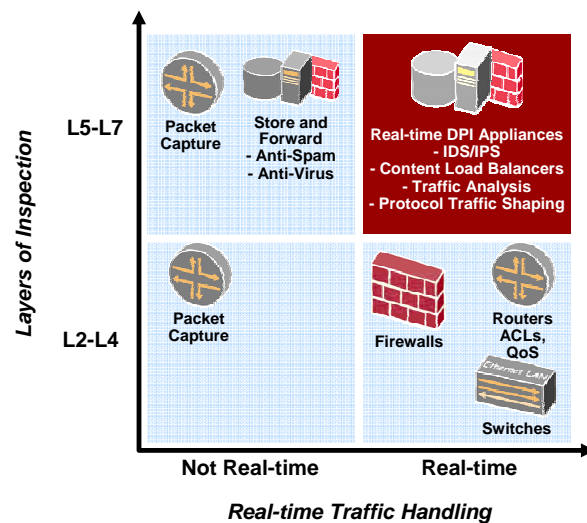
16

DPI-introduced Challenges

- /// Finer granularity → vast increase in compute power
- /// Increased options for data manipulation → flexibility
- /// Changing networking environment → extensibility
- /// Application and protocol diversity → customizability

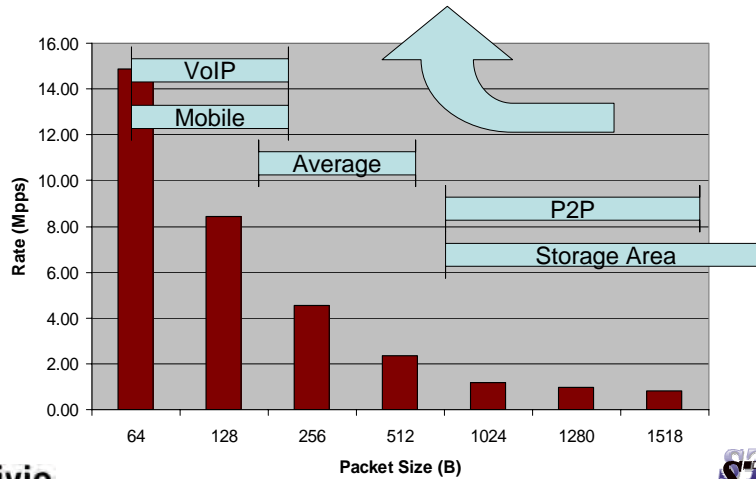
High compute/high throughput networking:
collision of computing and networking is the key dynamic for next generation networking

DPI Hardware Implementations



10 Gbps Considerations

- ⚡ DPI performance significantly harder to maintain at 10 Gbps speeds
- ⚡ Network applications drive overall network impact



Real-time DPI Devices

- ⚡ Enable real-time, inline inspection, analysis and control
- ⚡ Requires significant processing capacity/density to perform L7 analysis at 10 Gbps speeds
- ⚡ Can be based on general-purpose CPUs
- ⚡ Can be based on custom hardware

Real-time DPI Devices

Advantages

- Capable of providing transparent real time L7 enforcement
- Purpose built architectures can provide high speed L7 capabilities

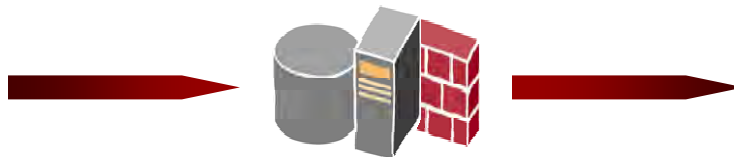
Disadvantages

- Hardware requirements greater than those of simple forwarding devices,
- Therefore, true 10G capable DPI platforms cost more than L3/L4 capable platforms

Achieving 10Gbps (Real-time)

Real-time DPI - Standalone form factor solutions

- Custom built appliances
- Servers with accelerator cards



Bivio Product Highlights

- ✦ **Unique system architecture optimized for wire-speed packet processing**
 - Powerful computation platform
 - De-coupling of network from CPU
 - Programmable data path
 - Hardware acceleration
- ✦ **Comprehensive software environment**
 - Standard Linux development environment
 - Multi-application support
 - Integrated management
 - High Availability & Redundancy
 - Clustering support
 - Advanced load distribution
- ✦ **Unique scaling capabilities enable true wire-speed for any service at 10 Gbps and beyond**
- ✦ **Fully Integrated Multi-Service/Multi-Application DPI Solutions**
 - Self-consistent, i.e., does not need any external system interaction to work
 - Extensive unified Logging and Data Correlation
 - Software-based: extensible and customizable



©2010 Bivio Networks, Inc.



23

Summary & Key Takeaways

- ✦ Internet is used daily for many business, personal & private aspects
- ✦ Threats are continuing to grow & evolve
- ✦ CNCI has allocated a plan & a budget to implement solutions throughout government agencies
- ✦ DPI platforms can be leveraged to solve challenging cyber security problems
- ✦ Bivio Networks is the leading supplier of open DPI platforms and cyber security solutions!



©2010 Bivio Networks, Inc.



24